Bitcoins, Blockchains and Cybersecurity

Dr. Debasis Bhattacharya, JD, DBA
debasisb@hawaii.edu
@uhmcabits
http://maui.hawaii.edu/cybersecurity
Online Transactions

• Physical cash
  – Non-traceable (well, mostly!)
  – Secure (mostly)
  – Low inflation

• Can’t be used online directly
  ➢ Electronic credit or debit transactions
    ◆ Bank sees all transactions
    ◆ Merchants can track/profile customers
E-Cash

• Secure
  – Single use
  – Reliable

• Low inflation

• Privacy-preserving
E-Cash Crypto Protocols

- Chaum82: blind signatures for e-cash
- Chaum88: retroactive double spender identification
- Brandis95: restricted blind signatures
- Camenisch05: compact offline e-cash

• Various practical issues:
  – Need for trusted central party
  – Computationally expensive
  – Etc.
Bitcoin

• A distributed, decentralized digital currency system

• Released by Satoshi Nakamoto 2008

• Effectively a bank run by an ad hoc network
  – Digital checks
  – A distributed transaction log
Size of the BitCoin Economy

• Number of BitCoins in circulation 16.5 million (September, 2017)
• Total number of BitCoins generated cannot exceed 21 million.
  – Around 5 million left to be mined!
• Average price of a Bitcoin:
  – $3867 on September 25, 2017;
  – $2350 on June 27, 2017
  □ Price has been very unstable and speculative.
• Currently, 244,157 tx/day or ~170 tx/minute. (In contrast, Visa transaction 200,000 per minute!)
# Blockchain Charts

The most trusted source for data on the bitcoin blockchain.

## POPULAR STATS

<table>
<thead>
<tr>
<th>Statistics</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Market Price (USD)</td>
<td>$3,904.48</td>
<td>USD</td>
</tr>
<tr>
<td>Average Block Size</td>
<td>0.96</td>
<td>Megabytes</td>
</tr>
<tr>
<td>Transactions per Day</td>
<td>244,157</td>
<td>Transactions</td>
</tr>
<tr>
<td>Mempool Size</td>
<td>10,810,666</td>
<td>Bytes</td>
</tr>
</tbody>
</table>

- Average USD market price across major bitcoin exchanges.
- The 24 hour average block size in MB.
- The aggregate number of confirmed Bitcoin transactions in the past 24 hours.
- The aggregate size of transactions waiting to be confirmed.
Bitcoins – Average price on September 25, 2017

GLOBAL BITCOIN PRICE INDEX (GBX) - Bitcoin (BTC) to United States Dollar (USD)

$3,867.63 USD

- -$61.98 (-1.58%)

Today's Open: $3,929.61
Today's High: $3,966.39
Today's Low: $3,755.90
USD Index: $3,859.29
24h Average: $3,876.50
Global Vol: $104329.72

3867.63 $ USD

3260.75 € EUR
25585.54 ¥ CNY
2868.71 £ GBP
Bitcoins – Average price since 2011
Bitcoins – Average price in 2017
Bitcoins in circulation

The total number of bitcoins that have already been mined; in other words, the current supply of bitcoins on the network.

Source: blockchain.info
Market Capitalization

The total USD value of bitcoin supply in circulation, as calculated by the daily average market price across major exchanges.

Source: blockchain.info
Transaction Rate

The number of Bitcoin transactions added to the mempool per second.

Source: blockchain.info
Average Number Of Transactions Per Block

The average number of transactions per block.

Source: blockchain.info
Bitcoin Block Reward Halving Countdown

Reward-Drop ETA date: 15 Jun 2020 07:22:45

The Bitcoin block mining reward halves every 210,000 blocks, the coin reward will decrease from 12.5 to 6.25 coins.

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Bitcoins in circulation</td>
<td>16,587,513</td>
</tr>
<tr>
<td>Total Bitcoins to ever be produced</td>
<td>21,000,000</td>
</tr>
<tr>
<td>Percentage of total Bitcoins mined</td>
<td>78.99%</td>
</tr>
<tr>
<td>Total Bitcoins left to mine</td>
<td>4,412,488</td>
</tr>
<tr>
<td>Total Bitcoins left to mine until next blockhalf</td>
<td>1,787,488</td>
</tr>
<tr>
<td>Bitcoin price (USD)</td>
<td>$3,863.80</td>
</tr>
<tr>
<td>Market capitalization (USD)</td>
<td>$64,090,830,797.50</td>
</tr>
<tr>
<td>Bitcoins generated per day</td>
<td>1,800</td>
</tr>
<tr>
<td>Bitcoin inflation rate per annum</td>
<td>4.04%</td>
</tr>
<tr>
<td>Bitcoin inflation rate per annum at next block halving event</td>
<td>1.80%</td>
</tr>
</tbody>
</table>
BitCoin: Challenges

• Creation of a virtual coin/note
  – How is it created in the first place?
  – How do you prevent inflation? (What prevents anyone from creating lots of coins?)

• Validation
  – Is the coin legit? (proof-of-work)
  – How do you prevent a coin from double-spending?

• Buyer and Seller protection in online transactions
  – Buyer pays, but the seller doesn’t deliver
  – Seller delivers, buyer pays, but the buyer makes a claim.

• Trust on third-parties
  – Rely on “proof of work” instead of trust
  – Verifiable by everyone – blockchain is visible to all
  – No central bank or clearing house
Security in Bitcoin

• Authentication
  – Am I paying the right person? Not some other impersonator?

• Integrity
  – Is the coin double-spent?
  – Can an attacker reverse or change transactions?

• Availability
  – Can I make a transaction anytime I want?

• Confidentiality
  – Are my transactions private? Anonymous?
Security in Bitcoin

• Authentication ➔ Public Key Crypto: Digital Signatures
  – Am I paying the right person? Not some other impersonator?

• Integrity ➔ Digital Signatures and Cryptographic Hash
  – Is the coin double-spent?
  – Can an attacker reverse or change transactions?

• Availability ➔ Broadcast messages to the P2P network
  – Can I make a transaction anytime I want?

• Confidentiality ➔ Pseudonymity
  – Are my transactions private? Anonymous?
Public Key Crypto: Encryption

- Key pair: public key and private key
Public Key Crypto: Digital Signature

- First, create a message digest using a cryptographic hash
- Then, encrypt the message digest with your private key
Cryptographic Hash Functions

• **Consistent:** hash(X) always yields same result
• **One-way:** given Y, hard to find X s.t. hash(X) = Y
• **Collision resistant:** given hash(W) = Z, hard to find X such that hash(X) = Z

Message of arbitrary length → Hash Fn → Fixed Size Hash
Back to BitCoin

• Validation
  – Is the coin legit? (proof-of-work) → Use of Cryptographic Hashes
  – How do you prevent a coin from double-spending? → Broadcast to all nodes

• Creation of a virtual coin/note
  – How is it created in the first place? → Provide incentives for miners, earn bitcoins after work!
  – How do you prevent inflation? (What prevents anyone from creating lots of coins?) → Limit the creation rate of the BitCoins. Right now, 12.5 coins to miners
Bitcoin

- Electronic coin == chain of digital signatures
- BitCoin transfer: Sign(Previous transaction + New owner’s public key)
- Anyone can verify (n-1)th owner transferred this to the nth owner.
- Anyone can follow the history

Given a BitCoin
Bitcoin Transactions

Public key 0xc7b2f68...

Public key 0xa8fc93875a972ea

Signature 0xa87g14632d452cd
Use of Cryptographic Hashes

- Proof-of-work
  - Block contains transactions to be validated and previous hash value.
  - Pick a nonce such that $H(\text{prev hash, nonce, Tx}) < E$. $E$ is a variable that the system specifies. Basically, this amounts to finding a hash value who’s leading bits are zero. The work required is exponential in the number of zero bits required.
  - Verification is easy. But proof-of-work is hard.
Preventing Double-spending

• The only way is to be aware of all transactions.
• Each node (miner) verifies that this is the first spending of the Bitcoin by the payer.
• Only when it is verified it generates the proof-of-work and attach it to the current chain.
Bitcoin Network

• Each P2P node runs the following algorithm:
  – New transactions are broadcast to all nodes.
  – Each node (miners) collects new transactions into a block.
  – Each node works on finding a proof-of-work for its block. *(Hard to do. Probabilistic. The one to finish early will probably win.)*
  – When a node finds a proof-of-work, it broadcasts the block to all nodes.
  – Nodes accept the block only if all transactions in it are valid *(digital signature checking)* and not already spent (check all the transactions).
  – Nodes express their acceptance by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.
Tie breaking

- Two nodes may find a correct block simultaneously.
  - Keep both and work on the first one
  - If one grows longer than the other, take the longer one

Two different block chains (or blocks) may satisfy the required proof-of-work.
Reverting is Hard

- Reverting gets exponentially hard as the chain grows.

1. Modify the transaction (revert or change the payer)
2. Recompute nonce
3. Recompute the next nonce
Practical Limitation

• At least 10 mins to verify a transaction.
  – Agree to pay
  – Wait for one block (10 mins) for the transaction to go through.
  – But, for a large transaction ($$$) wait longer, around 60 minutes. Because if you wait longer it becomes more secure.
  – For large $$$, you wait for six blocks (1 hour).
Optimizations

- Merkle Tree
  - Only keep the root hash
    - Delete the interior hash values to save disk
    - Block header only contains the root hash
    - Block header is about 80 bytes
    - 80 bytes * 6 per/hr * 24 hrs * 365 = 4.2 MB/year
  - Why keep use a Merkle tree?
Simplified payment verification

- Any user can verify a transaction easily by asking a node.
- First, get the longest proof-of-work chain
- Query the block that the transaction to be verified (tx3) is in.
- Only need Hash01 and Hash2 to verify; not the entire Tx’s.
BitCoin Economics

- Rate limiting on the creation of a new block
  - Adapt to the “network’s capacity”
  - A block created every 10 mins (six blocks every hour)
    - How? Difficulty is adjusted every two weeks to keep the rate fixed as capacity/computing power increases

- N new Bitcoins per each new block: credited to the miner
  - Incentives for miners
    - N was 50 initially. In 2013, N=25
    - Since 2016 N = 12.5, next half is June 2020 for N = 6.25.
    - Halved every 210,000 blocks (every four years)
    - Thus, the total number of BitCoins will not exceed 21 million.
      (After this miner takes a fee)
Privacy Implications

• No anonymity, only pseudonymity
• All transactions remain on the block chain—indefinitely!
• Retroactive data mining
  – Target used data mining on customer purchases to identify pregnant women and target ads at them (NYT 2012), ended up informing a woman’s father that his teenage daughter was pregnant
  – Imagine what credit card companies could do with the data
THE INSIDE STORY OF MT. GOX, BITCOIN'S $460 MILLION DISASTER
Bitcoins – Average price dropped in 2014 but rising since!
Powerful Bitcoin and Bitcoin Cash wallet

Send, receive, and store your funds securely with BTC.com’s wallet.

Create new wallet

Already have a wallet?

Email

Password

I agree to the terms of service
One Wallet For Your Digital Life

Send and receive bitcoin easily and securely

Maintain full control over your bitcoin private keys

Pay friends without QR codes or long addresses
BUY AND SELL DIGITAL CURRENCY

Coinbase is the world’s most popular way to buy and sell bitcoin, ethereum, and litecoin.

Enter your email address

Get Started

New to bitcoin? | What is ethereum?
47,000 Businesses Trust Coinbase To Integrate Bitcoin Payments, Including...

- mint.com
- CheapAir.com
- KHAN ACADEMY
- overstock.com
- intuit
- PayPal
- United Way
- USAA
- WIKIMEDIA FOUNDATION
- Time Inc.
- REEDS Jewelers
- 1-800-flowers.com
- Expedia
- FIDELITY Charitable
- Bloomberg
- dish
- Mozilla
- Bing
How to lose $8k worth of bitcoin in 15 minutes with Verizon and Coinbase.com

It begins with a text message from Verizon

11:31 PM

Free VZW Msg: You're on the phone with Verizon and just authenticated with an alternative method. Not you?
Coinbase Exits as Hawaii Requires Bitcoin Companies to Hold Fiat Reserves
How is Coinbase insured?

Aug 11, 2017

Coinbase holds less than 2% of customer funds online. The rest is held in offline storage.

This insurance policy does not cover any losses resulting from the compromise of your individual Coinbase account. It is your responsibility to use a strong password and maintain control of all login credentials you use to access Coinbase and GDAX.

Fiat Currency

Coinbase stores all customer fiat currency (government-issued currency) in segregated, custodial bank accounts. The funds held in those accounts belong to Coinbase’s customers - not to Coinbase.

If you are a United States resident, your Coinbase USD Wallet is covered by FDIC insurance, up to a maximum of $250,000.

Even if Coinbase were to become insolvent, the funds held in the custodial bank accounts could not be claimed by Coinbase or its creditors. The funds held in those accounts would be returnable to Coinbase’s customers.
Bitcoin Security 101

• When using an online service such as an bitcoin exchange such as Coinbase:
  – Enable 2-Factor-Authentication (like Google authenticator or YubiKey) on your account
  – Watch out for Social Engineering that can take switch your phone by calling Verizon Customer Svc!

• Ensure security of your API Key
  – API Key allows applications to retrieve bitcoins from your digital wallet.
Security Best Practices

Storing Credentials Securely

You should take great care to store your credentials securely. If someone obtains your `api_secret` with the `wallet:transactions:send` permission, they will be able to send all the digital currency out of your account.

You should avoid storing API keys in your code base (which gets added to version control). The recommended best practice is to store them in environment variables. Learn more about environment variables here. Separating credentials from your code base and database is always good practice.

Validating SSL Certificates

It is also very important that your application validates our SSL certificate when it connects over `https`. This helps prevent a *man in the middle attack*. If you are using a client library, this may be turned on by default, but you should confirm this. Whenever you see ‘verify SSL’ you should always ensure it is set to true.

Additional Security for API Keys

For enhanced API Key security, we recommend that you whitelist IP addresses that are permitted to make requests with a particular API Key.
Bitcoin Security 101

- Always have direct control of your bitcoins (private keys). If you don’t have (or lose) the keys, you don’t control the bitcoins.
- Keep little cash ($100 to $500) in the exchange
- Make regular backups of your bitcoin wallet!
  - Or, use Trezor hardware wallet or paper wallet
- Realize that you will be the target for malware, social engineering and other hacks!
Satoshi Labs

Trezor Hardware Wallet for Bitcoin, Dash, Litecoin, Zcash, Ether Bundle with OTG Cable for Android Devices - black

Be the first to review this item

Price: $129.00 prime

Earn $6.45 by choosing 5% back with the Amazon Prime Store Card.

Only 15 left in stock - order soon.

Sold by nkmtouS and Fulfilled by Amazon. Gift-wrap available.

- The most trusted and secure way to store your Bitcoins, Dash, Litecoin, Zcash and Ether (via MyEtherWallet)
- Isolate your private keys into the safety of TREZOR and enjoy Bitcoin without risk.
- TREZOR is a USB 2.0 device compatible with Windows, Linux and OS X (10.8 or higher).
- This bundle includes original OTG cable (MicroUSB to MicroUSB) for use with Android devices. Compatible with all Android devices supporting USB host.
Private bank in your hands.

TREZOR Wallet is an easy-to-use interface for your TREZOR device. From this Wallet, you can easily control your coins, manage your balance and initiate transfers.

Install TREZOR Chrome Extension to allow TREZOR Wallet to talk with your device.

Don’t have a TREZOR? Get one >
Ledger Nano S

Ledger Nano S Cryptocurrency Hardware Wallet

Price: $84.88 ✅prime

Get $70 off instantly: Pay $14.88 upon approval for the Amazon Prime Rewards Visa Card.

Note: Available at a lower price from other sellers, potentially without free Prime shipping.

In Stock.
Want it Thursday, Sept. 28? Order within 32 hrs 17 mins and choose Priority Shipping at checkout. Details

Sold by E Vigilia and Fulfilled by Amazon. Gift-wrap available.

- Check and confirm transactions on the display and confirm with using the physical buttons (anti-malware second factor)
- Your confidential data is never exposed: it is secured inside a strongly isolated environment locked by a PIN code
- Use companion apps such as cryptocurrencies wallets, and also FIDO U2F, GPG, SSH or build your own applications
- Ledger Nano S supports the FIDO Universal Second Factor authentication standard on Google, Dropbox, GitHub or Dashlane
- Your accounts are backed up on a recovery sheet. Easy restoration on any Ledger device or compatible wallets (BIP39/BIP44)
Conclusion

• Cryptocurrencies and technology are here to stay…
  – www.Bitcoin.org - Started by Satoshi Nakamoto, 10/08
  – www.ZeroCoin.org - Extend Bitcoin to make it private
  – www.Ethereum.org - Smart Contracts (Microsoft)
  – www.Hyperledger.org - Blockchains for Business (IBM)

• Security is an issue just like anything else
  – Consumers: Social Engineering, Malware, Phishing etc.
  – Exchanges: Hacks, Botnets, Malware, Phishing, APT etc.
Acknowledgement

• Some of the slides, content, or pictures are borrowed from the following resources, and some pictures are obtained through Google search without being referenced below:

• [L24-BitCoin and Security](#), many of the slides borrowed from this presentation with modifications.

• Presentation by Amir Houmansadr from Umass CS entitled “Secure Digital Currency: Bitcoin”, CS660, Spring 2015
Dr. Debasis Bhattacharya, JD, DBA

debasisb@hawaii.edu

@uhmcabit

http://maui.hawaii.edu/cybersecurity